

**SPOOFING, PHISHING AND IDENTITY THEFT:
TIPS FOR AVOIDING ACCIDENTAL INVOLVEMENT WITH THEFT AND FRAUD**

October 7, 2005

RECENT DEVELOPMENTS IN INTERNET SELLING AND ADVERTISING

**LAW SEMINARS INTERNATIONAL
STATE BAR OF CALIFORNIA BUSINESS LAW SECTION**

Maureen A. Young

Bingham McCutchen LLP

(415) 393-2788

Maureen.Young@Bingham.com

© 2005 Maureen A. Young - All rights reserved

BINGHAM McCUTCHEN

I. Overview: The Growth of Cybercrime

The expansion of ecommerce and online data collection has attracted a new brand of criminals deploying diverse and ever changing schemes for cybercrimes, including spoofing, phishing, pharming, and various identity theft scams. While these cybercrimes are similar to older theft and fraud scams that in past years may have been deployed by phone or mail or in person, the online nature of the cybercrimes has made them more prevalent and harder to track down and resolve.

A. Characteristics of Cybercrime:

- Many variations, but all part of the same problem.**
- Schemes change quickly.**

- **Although companies may respond by deploying security technology fixes for the problems, the bad guys quickly find new ways to get around the technology fixes.**
- **Anonymity of the Internet: Servers may be identified, but the real persons behind the servers may not be readily identified.**
- **Enforcement issues: Difficulty of obtaining long-arm jurisdiction and cooperation of local law enforcement in certain foreign countries. Culprits often offshore in countries with less rigorous criminal and tort law enforcement regimes.**

B. Many Types of Scams:

- **Phishing - “fishing” for confidential information through phony means - general term for criminals’ creation and use of emails and websites designed to look like emails and websites of legitimate businesses, including financial institutions and**

government agencies, in order to fraudulently obtain and use an individual's personal or financial information.

- **Pharming - redirection of an individual to an illegitimate website through technical means. E.g., an Internet banking customer, who routinely logs into his online banking website may be directed to an illegitimate website instead of accessing his bank's website. Often completed by the criminal using cookies, code or other technical means to physically redirect ("hijack") the user to the illegitimate website. A hacker may be able to engage in domain hijacking by redirecting all of company's legitimate Internet traffic to an illegitimate site.**
- **Spoofing - actually a variation of pharming, sometimes known as static domain name spoofing, in which the criminal attempts to take advantage of slight misspellings in a company's domain**

name or close approximations of a company's domain name to trick users into inadvertently visiting the wrong site. The criminal's site will attempt to create the look and feel, logo, layout, etc. of the official site so that the user is duped into thinking that he is visiting the official site. For example, a user trying to reach anybank.com, may type in by mistake a misspelling, e.g., anybnk.com, or a close cousin of the domain name, e.g., anyusbank.com, and not realize that he is not visiting the official site of his bank.

- **Identity Theft - runs the gambit of a thief fraudulently using someone else's credit card number to a criminal assuming the full identity of an individual. Extraordinary consumer concern over identity theft because of the high incidence of information security breaches.**

C. Varied Motives of Cybercriminals:

- **Money, money, money - derived from fraudulent use of personal and financial information and/or selling that information on the black market. Cybercrime has been used to facilitate organized criminal networks, money laundering and terrorism.**
- **Malicious intent - install malware, including viruses and Trojans, to destroy a company's or user's system.**
- **Cheap thrills - ability to hack and disrupt prominent systems and databases. E.g., students hacking into U.C. Berkeley's system.**

D. Corporate and Governmental Reaction:

- **Efforts by companies to create new security technologies and procedures, including virus detection software, enhanced**

firewalls, spyware scanning tools, greater deployment of encryption, new security procedures to authenticate the user, better development of corporate information security plans, and employee and user training.

- **Governmental agencies - huge effort by the key regulatory agencies (notably, the FTC, FDIC and DOJ) to educate consumers and businesses through issuing guidance and guidelines about how to identify and protect themselves against cybercrimes.**
- **Legislative efforts - many identity theft, data protection and other cyber-related bills introduced at the federal and state levels.**
- **Law enforcement - efforts to deploy special enforcement units to focus on the cybercrime, e.g., U.S. Attorney's Office Computer Hacking and Intellectual Property ("CHIP") unit.**

II. A Closer Look at Phishing

A. Some key points:

- **Said to be the fastest growing cybercrime.**
- **Phishing uses both social engineering and technical subterfuge to steal consumers' personal identity data and financial account information.**
- **In one of the most common phishing scams, the fraudulent email message will request that recipients update or validate their financial or personal information in order to maintain their accounts. The user is directed to a fraudulent site that will look very similar to the legitimate site to enter personal information.**
- **Although many industry sectors have been affected by phishing, the financial services industry has been most heavily hit.**

- **The Anti-Phishing Working Group, www.antiphishing.org, is one of the leading groups of industry and law enforcement entities trying to alert the business and law enforcement community to particular phishing scams and to formulate industry responses to phishing. Also, the Financial Services Technology Consortium (“FSTC”) has launched a counter-phishing initiative to: share knowledge about phishing scams; conduct pilot responses to phishing attacks; and recommend and deploy industry-wide solutions.**

B. FTC/DOJ Guidance to Consumers:

- **DOJ: Stop, Look and Call.**
- **If you get an email or pop-up messages that asks for personal or financial information, do not reply and don’t click on the link in**

the message. Never provide your personal information to an unsolicited request.

- **Use anti-virus software and a firewall, and keep them up to date.**
- **Don't email personal or financial information.**
- **Review credit card and bank account statements as soon as you receive them.**
- **Be cautious about opening any attachment or downloading any files from emails.**
- **Forward/report spam that is phishing for information to the company being impersonated.**
- **If you believe you have been scammed, file a report with law enforcement and a complaint with the FTC. Place fraud alerts on your credit files.**

C. FDIC Guidance for Financial Institutions:

- **Issued two studies - the first in December, 2004, which was supplemented by another report in June, 2005.**
- **Urged financial institutions to:**
 - (i) Educate consumers about protecting themselves from phishing scams;**
 - (ii) Develop enhanced incident response programs to fraud schemes; and**
 - (iii) Take actions to mitigate risk associated with email and Internet-related fraudulent schemes.**
- **Consumer education should include notification through statement stuffers and posting notices on the financial institution's website informing customers that:**
 - **A financial institution's webpage should never be accessed from a link provided by a third party. It should only be**

accessed by typing the website name or URL address directly into the web browser or by using a bookmark to get to the site.

- The financial institution will not send email messages that request confidential information, such as account numbers, passwords or PINs. Customers should report any such requests to the institution.**
- The financial institution maintains current website certificates. Describe how the customer can authenticate the institution's webpages by checking the properties on a secure webpage.**
- Enhancements of incident response programs may include:**
 - Incorporating notification procedures to alert customers of known email and Internet-related fraudulent schemes, cautioning them not to respond.**
 - Establishing a process to notify Internet service providers, domain-name issuing companies, and law enforcement to**

shut down fraudulent websites and other Internet resources that may be used to facilitate phishing or other fraudulent schemes.

- Offering customers assistance when fraud is detected in connection with customer accounts.**
- Notifying the proper authorities when email and Internet fraudulent schemes are detected, including notifying the appropriate regulatory agencies and law enforcement agencies.**
- Filing Suspicious Activity Reports (“SARs”) when incidents are suspected.**
- Steps to mitigate risks associated with email and Internet-related fraudulent Schemes may include:**
 - Improving authentication methods and procedures to protect against the risk of user ID and password theft.**
 - Reviewing and, if necessary, enhancing practices for protecting confidential customer data.**

- **Increasing suspicious activity monitoring and employing additional identity verification controls. Monitor accounts individually and in the aggregate for unusual account activity such as address or phone number changes, a high volume of transfers, and unusual customer service requests.**
- **Establishing a toll-free number for customers to verify requests for confidential information or to report suspicious email messages.**
- **Training customer service staff to refer customer concerns regarding suspicious email requests to internal security staff.**

D. User Name and Password Protection No Longer Enough:

- **Importance of the FDIC studies -- they conclude that it is no longer sufficient for institutions to protect remote access to accounts through using only user name and passwords. Instead, the FDIC endorsed supplementing existing user name/password**

procedures, using “multifactor” authentication and other “layered” security procedures.

- Interagency banking guidance likely to be issued within the next few weeks which will require financial institutions to meet certain deadlines for deploying multifactor authentication processes.**
- This means that companies such as PassMark Security, which offers two-factor, two-way authentication systems, are likely to find their services in high demand. PassMark utilizes challenge questions and secure non-intrusive cookies to identify user device/server/location; once authenticated, it presents the user with his pre-selected secret “passmark,” so he can then enter his password with confidence that he is entering the legitimate website. PassMark Security recently entered into a major agreement with Bank of America.**

- **Because of the magnitude of the phishing problems, companies have been given some legal leeway to block suspected phishing sites. For example, a court recently found Earthlink to be not liable for blocking emails from Associated Bank's site, even though Earthlink incorrectly identified Associated Bank's site as a phisher's site.**

E. Legislative Efforts:

- **California's SB 355 (Murray), "The Anti-Phishing Act of 2005," is enrolled, awaiting the Governor's signature. Makes it unlawful for any person, through the Internet or other electronic means, to solicit, request, or take any action to induce another person to provide identifying information by representing itself to be a business without the approval or authority of that business. Business may recover the greater of actual damages or**

\$500,000. Individual may recover the greater of three times actual damages or \$5000 per violation. Attorney General may seek civil penalties of up to \$2500 per violation.

III. Additional Points on Pharming and Spoofing

A. Pharming:

- Importance of legitimate sites using digital certificates to differentiate themselves from illegitimate sites. Consumers can use the certificate as a tool to determine whether a site is trustworthy. Take prompt responses to any signs, such as decreased traffic, of domain name server (“DNS”) poisoning, which can occur as a result of misconfiguration, network vulnerabilities or malware installed on the server.**

B. Spoofing:

- **Companies should monitor for fraudulent websites using variations of the company's name.**
- **Companies need to diligently manage their domain names by ensuring that domain names are renewed in a timely manner. They should investigate the possibility of registering similar domain names. In addition, many registrars offer domain locks (i.e., no transfers unless unlocked) to prevent unauthorized domain slamming.**
- **Difficulties with taking the spoofed site down if the company has no domain name rights to the spoofed variation. Formal appeal to domain registrars takes a long time; law enforcement may not be effective if the server is offshore. Civil action may result in no response by the plaintiff.**

V. Identity Theft: A Vast and Pervasive Problem

Identity theft crimes have been around for a long time (e.g., unauthorized access and misuse of information obtained through phone calls, tampering with mail, and plain old pickpocketing), but the online collection and electronic storage of data have led to new problems with identity theft. Identity theft has been facilitated by the large scale incidents of security breach that have been so prevalent in the last years.

A. The Value of Regulatory Guidance for Consumer and Business Education:

- The key regulatory agencies, including the FTC, FDIC, DOJ and the FBI, have aggressively issued consumer alerts and guidance for businesses in the area of identity theft, phishing, pharming and other cybercrimes. Notably, the FTC issued its booklet,**

“Take Charge: Fighting Back Against Identity Theft,” which serves as a self-help guide for consumers affected by identity theft. (The booklet is included in your materials.) The FTC also recently launched its new consumer information website, **OnGuardOnline.gov**.

- **To briefly summarize, the FTC has advised consumers to protect themselves against identity theft by:**
 - **Protecting Social Security numbers, financial account and credit card numbers, PINs, passwords and other financial and personal information.**
 - **Keeping financial trash “clean.”**
 - **Using extra care before providing personal information over the Internet.**
 - **Becoming more wary of free offers and other opportunities “too good to be true.”**

- **If a consumer believes he has fallen victim to identity theft, the FTC recommends that the consumer:**
 - **Check all accounts with card issuers and financial institutions.**
 - **If unauthorized charges appear, report them and request that accounts be closed and new cards issued.**
 - **Write letters to creditors and others requesting that unauthorized charges be removed or inaccurate information corrected.**
 - **Place a credit alert on one's credit files.**
 - **Continue to closely check one's credit report and all card and financial statements regularly for years after the identity theft occurred.**
 - **Report the incident to law enforcement and file a complaint with the FTC.**
 - **Consider obtaining a credit monitoring service and/or identity theft insurance.**

B. Identity Theft Has Been Facilitated by Large Scale Data Security Breaches:

As you know, we have witnessed a rash of recent information security breaches, including the CardSystems Solutions, ChoicePoint, Citibank, BofA, Lexis/Nexis, DSW, Time Warner, Iron Mountain, the Hackensack scam, and other incidents. The security breaches have occurred as a result of varied weaknesses in companies' information security policies and procedures, including as a result of:

- Hacking into the company's databases;**
- Thefts (stolen laptops);**
- Mishaps in the physical handling of information (data tapes lost in transit, lost laptops);**

- **Employee wrongdoing (selling customer information to identity thieves and others);**
- **Failures in controls over access to information (failure to properly screen background of persons allowed to acquire or access personal information);**
- **Any of the above occurring at the service providers maintaining the company's customers' information; and**
- **Particular problems with loss and theft of records at document storage vendors.**

The high incidence of security breaches has resulted in heightened concern over the protection of confidential consumer information, which has led to a spate of new proposed federal and state legislation.

C. Key Legislative and Regulatory Developments:

- **GLBA Requirements.** Regulations applicable to financial institutions on Safeguarding Customer Information were promulgated in 2001 pursuant to the Gramm-Leach-Bliley Act (“GLBA”) of 1999. They require a financial institution, including its subsidiaries, to implement a comprehensive written information security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the financial institution and the nature and scope of its activities. The information security program must be designed to:
 - (i) Ensure the security and confidentiality of customer information;
 - (ii) Protect against any anticipated threats or hazards to the security or integrity of such information; and

- (iii) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.**
 - Involvement of the Board of Directors is required, including the Board's review and approval of the institution's written information security program and thereafter, at least annual reviews.**
 - Institutions are also required to ensure that their service providers, as well as their service providers' subcontractors, are subject to written information security plans.**
- Final Interagency Guidance on Response Programs for Security Breaches - issued by the banking regulatory agencies in March, 2005. See, Interagency Guidance with full commentary at <http://www.fdic.gov/news/press/2005/pr2605.html>. Under the Interagency Guidance, each financial institution must develop and implement a written risk-based response program to**

address incidents of unauthorized access to customer information. The response program should be a key part of the institution's information security program.

- **California Law. States became active in this area, notably with California's enactment of SB 1386 (the Peace legislation), California Civil Code 1798.82:**
 - **Requires that any company that conducts business in California and owns or licenses computerized data that include personal information about the California residents must disclose any breach of the security of the computerized data to the consumer whose “unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”**
 - **Companies that maintain such information on behalf of other companies have to promptly notify the owner or licensee of the information of any potential breach.**

- The notice can be delayed if a law enforcement agency determines that the notification will impede the related criminal investigation.
- Written notice, or email notice consistent with the E-Sign, has to be given to the consumer.
- Substitute notice (including a website posting with notice to statewide media) can be given if sending the individual written notice will cost more than \$250,000 or the number of persons affected exceeds 500,000.
- A company can also use “alternative notice” if it maintains its own reasonable notification procedures as part of an information security policy/plan. *[Note: Because financial institutions are required by GLBA to have information security plans that include incident response programs, financial institutions should be able to utilize this alternative notification provision.]*

- Under the Act, affected customers may sue to recover damages, businesses that violate the Act may be enjoined, and other rights and remedies are available under the law.
- **Guidance from the California Office of Privacy Protection.** The California legislation did not specify the particulars of the required notice, but the California Office of Privacy Protection did issue Recommended Practices. See, <http://www.privacy.ca.gov/recommendations/secbreach.pdf>.
 - A typical information security breach notice would include a description of the nature of the incident, status of the investigation, identification of the risk to the consumer, recommendation that the consumer put a fraud alert on their consumer credit accounts by contacting one of the three consumer reporting agencies, provision of the phone numbers for those agencies, recommendation that the consumer check his accounts for the next few years, and

- information on how to contact the company and the CA Office of Privacy Protection, etc. to obtain more information.**
- **Information security notices after the enactment of the Peace legislation became very stylized, although companies made their own decisions of what additional “goodwill offerings” (e.g., one year of free credit monitoring, access to free credit counseling) to provide to affected consumers.**
 - **Post-Peace Reaction. After the Peace legislation was enacted, companies around the country with California customers struggled with their decisions on whether to give the notice or not in certain breach circumstances. Consideration was given to whether the breach:**
 - **Really was of “computerized data;”**
 - **If “unauthorized access” to the information had really occurred;**

- If the company really had a “reason to believe” that unauthorized access had occurred;
 - How soon after the incident the company should give notice; and
 - If the notice was given, how the notice would impact the company’s business reputation.
- **Other States Also Enacted Security Breach Notification Legislation.** In addition to California, at least another 21 states have enacted some form of security breach notification legislation including Alaska, Arkansas, Connecticut, Delaware, Florida, Georgia, Illinois, Indiana, Louisiana, Maine, Minnesota, Montana, Nevada, New Jersey, New York, North Carolina, North Dakota, Rhode Island, Tennessee, Texas and Washington. Security breach notification legislation was introduced in at least another 13 states this year.

- **FTC Actions.** The FTC also issued recommended guidance to businesses on information security breach -- the recommendations track the California Office of Privacy Protection's guidance. See, <http://www.ftc.gov/bcp/online/pubs/buspubs/idthrespond.htm>. The FTC also issued warnings that it viewed negligent security standards, resulting in harm to consumers, as an “unfair and deceptive” business practice for which the FTC may take enforcement action under Section 5(a). The FTC has subsequently brought such enforcement actions.
- **California's AB 1950.** Last year, California enacted AB 1950, which requires that all companies doing business in California, *and their subcontractors*, adopt reasonable security procedures and practices. What counts as “reasonable” security procedures is not further defined, leaving companies to independently

determine what are reasonable means. Best to assume that it imposes at least requirements similar to those required under the GLBA.

- **Federal Legislation. Many, many competing bills were introduced this year in the security breach/identity theft area. Several bills are currently “leading” in Congressional attention:**
 - **S. 1408, Stevens/Inouye, the “Identity Theft Protection Act.” Would require companies to notify consumers when their personal information is compromised if there is a “reasonable risk” of identity theft. [N.B.: Consumer groups oppose this bill because they view the “reasonable risk” standard as too narrow to protect consumers.]**
 - **S. 1789, Specter/Leahy, the “Personal Data Privacy and Security Act.” Would require companies to notify consumers about data breaches involving their personal information and to implement data privacy and security**

programs. A company, after conducting a risk assessment, could determine that notice to the consumer is not necessary if there is no “significant risk” of identity theft. The bill would also increase criminal penalties for identity theft and allow consumers access to, and the opportunity to correct, any personal information held by data brokers (post-ChoicePoint concerns). The bill also requires the government to establish rules protecting privacy and security when it uses data broker information and imposes penalties on government contractors that fail to comply with such rules.

- House Commerce Staff Discussion Draft, Barton/Dingell. Would require notification when a consumer’s personal information is “acquired” by an unauthorized person as a result of a security breach. The FTC would define, by regulation, what constitutes a “security breach” for purposes of notifying consumers. At a minimum, a breach would**

mean there is a “reasonable basis” to conclude that identity theft could result.

- **S. 751, Senator Feinstein, “Notification of Risk to Personal Data Act.” Attempts to nationalize the requirements of California’s existing legislation, but would apply whether or not the data is held in electronic form. Also provides for civil penalties of up to \$1000 per individual affected and not more than \$50,000 per day while the failure to give the required notice persists.**
- **California Legislation. Two key bills died this year, but may reappear next year in some form:**
 - **SB 852, Bowen. Would have amended the Peace legislation to have it apply to breaches of both computerized data and data not held in electronic form. Would be preempted by the federal bill S.751, if enacted.**

- **SB 550, Speier.** In its original form, would have enacted measures allowing consumers to access their personal information held by data brokers, and allowing them to ask that errors be corrected.
- **Other Legal and Regulatory Developments.**
 - **GLBA standard for All?** FTC Chairman Majoras has recommended to Congress that the GLBA Safeguarding Regulations be imposed on all companies, not just financial institutions.
 - **Rules on Proper Disposal of Customer Information.** The federal banking agencies and the FTC issued final rules on the proper disposal of customer information and records, requiring companies to take “reasonable measures” to protect against unauthorized access to or use of customer information in connection with its disposal.

- **The FDIC issued in June, 2005 Guidance on Developing an Effective Pre-Employment Background Screening Process - The financial institution's process should, at a minimum, uncover information regarding a job applicant's convictions, verify the applicant's identity, determine if the applicant's submitted information is true and correct, and determine whether any consent to hire the candidate may be necessary from the regulatory agency. Institutions must verify that the employees of their subcontractors are subject to similar screening procedures as those deployed by the institution.**
- **FCRA/FACT Act Regulatory Developments. The Fair and Accurate Credit Transactions Act (the "FACT Act") was enacted in 2003, amending the Fair Credit Reporting Act ("FCRA"), 15 USC Section 1681 et seq. The FACT Act includes many new requirements on consumer reporting agencies and on companies that use consumer reports or furnish information to consumer reporting agencies, which**

are designed to prevent and mitigate the effects of identity theft, including requiring specified responses to fraud alerts and requirements that companies implement “red flag” guidelines to prevent identity theft. The “red flag” regulations are expected to be proposed soon.

- Payment Card Industry (“PCI”) Data Security Standards. As of June 1, 2005, Visa, Mastercard and the consortium of other major payment card companies are requiring all online retailers (not just major retailers) that accept credit and debit cards to submit to certain validation processes to ensure that they are meeting the mandatory standards for handling customer data. To be certified under the PCI Data Security Standards, all merchants who process purchases made with cards from American Express, Diners Club, Discover, JCB International Credit Card, MasterCard and Visa must comply with the PCI’s 12-step security audit standards. See, www.visa.com.**

VI. What Companies Should Be Doing Now

Unfortunately, the increasing incidence of cybercrime and security breach has resulted in more regulation of and greater liability on companies collecting confidential consumer data. Companies need to reassess and enhance existing security practices and procedures:

- Conduct thorough risk assessment and amend existing security plans in light of laws and regulations recently adopted -- e.g., develop improved procedures for: incident response/customer notice, disposal of customer information and records, enhanced employee background screening procedures, handling of fraud alerts, addressing red flags for identity theft, shipping data in a secure fashion, etc.**

- **Particularly examine your company's data collection and retention practices and determine if all the data currently collected and retained is really necessary for operations. If not, collect less and determine when and how data retained can be destroyed.**
- **Review employee policies and make sure they are up to date -- for example, what controls does your company have in place regarding hand-held devices (fobs, etc.), use of laptops, camera phones, physical and electronic access to customer confidential data, etc.**
- **Adopt appropriate new technologies to protect against cybercrime, including deploying multi-factor authentication for remote access, greater use of encryption and truncation, anti-spyware software, enhanced firewalls, etc.**

- **Consider having an independent security audit conducted to identify weaknesses and then deploy enhancements to your security program accordingly.**
- **Stay abreast of the changing nature of the cybercrime and educate/train customers and employees regularly.**
- **Enhanced Vendor Management: Review existing contracts with vendors and update/amend contractual requirements. Make sure that you have recently reviewed a copy of each vendor's information security plan and that the plan is up to date with current requirements. Audit the vendor's operations as necessary for security protection.**
- **Develop a “culture of privacy” throughout the corporation -- apply privacy principles at every step of the information life cycle, from collection and use through to disclosure and disposal.**